Active Directory - Méthode AGDLP

Difficulté : Débutant

Notions : Active directory, Organisation, Bonne pratique, méthodologie AGDLP.

I. Introduction

La méthode AGDLP (**A**ccount **G**lobal **D**omain **L**ocal **P**ermission) est une méthode de gestion de droits et permissions à travers les groupes Active Directory et plus largement LDAP.

Cette méthode poursuit un objectif triple :

- **Management** : Cela facilite la délégation des accès et de la gestion de ceux-ci. Le fait de dé-corréler l'utilisateur de ses droits d'accès rends la solution scalable et facilement réversible.

- **Audit / Respect RGPD** : Elle aide également à la conformité RGPD car grâce à elle, il deviens facile et rapide de savoir avec précision qui a accès à quoi. Cela rends la traçabilité plus simple et précise.

- **Cyber sécurité / Moindre privilège** : Elle permet enfin de s'assurer une normalisation des droits d'accès en s'assurant que chaque utilisateur dispose uniquement des droits strictement nécessaires et que la portée de ces droits est correctement ajustée.

La combinaison de ces trois buts résulte en une gestion qui a priori peut sembler complexe à la mise en oeuvre, mais qui se révélera par la suite bien plus simple, transparente et efficiente dans son utilisation courante.

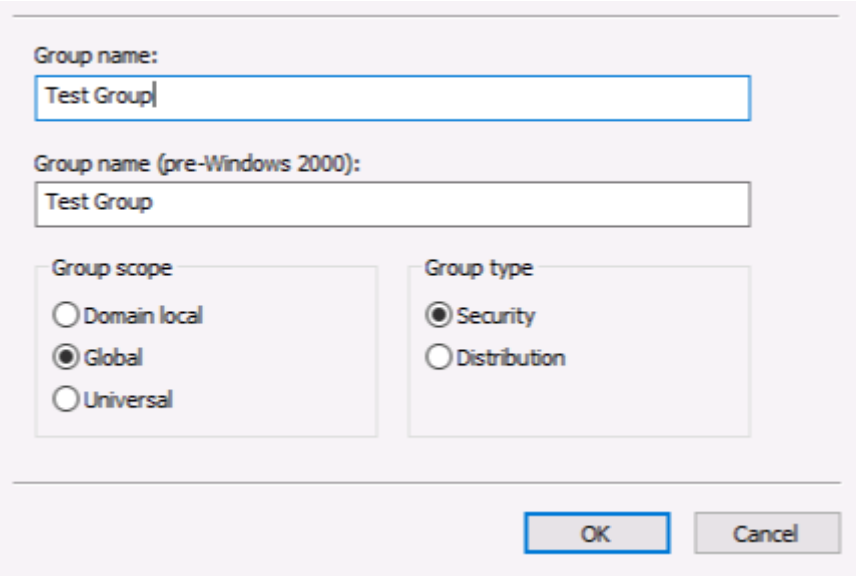
Dans un second temps, il deviendra aussi possible d'encadrer correctement la délégation de la gestion des accès et des privilèges.

Cette méthode peux s'appliquer indépendamment aux serveurs de fichiers, aux différents services et applications de l'entreprise, ainsi que (par le biais du SSO) aux rôles des application fédérées.

> **Info** : Cette méthode prends tout son sens dans un environnement multi-domaines comme c'est de plus en plus fréquent d'en voir avec la logique de tiering.

II. Rappel : Portée des groupes AD

Avant de rentrer plus en détail sur l'application de cette méthode, il est nécessaire de rappeler certaines bases du fonctionnement des groupes Active Directory (ou LDAP) car c'est sur eux que va intégralement s'appuyer cette méthode.



Pour rappel, il exite deux types de groupes :

- **Security** (sécurité) : Ce type de groupe est celui qui va être utilisé dans ce contexte. C'est celui qui permet de gérer les permissions et les droits d'accès ainsi que l'application des GPO.
- **Distribution** : Ce type de groupe sert à gérer les listes de distribution pour les mails.

A cela s'ajoute la portée du groupe. c'est ce point qui va être central dans l'utilisation d'AGDLP. Il s'agit du niveau de visibilité du groupe.

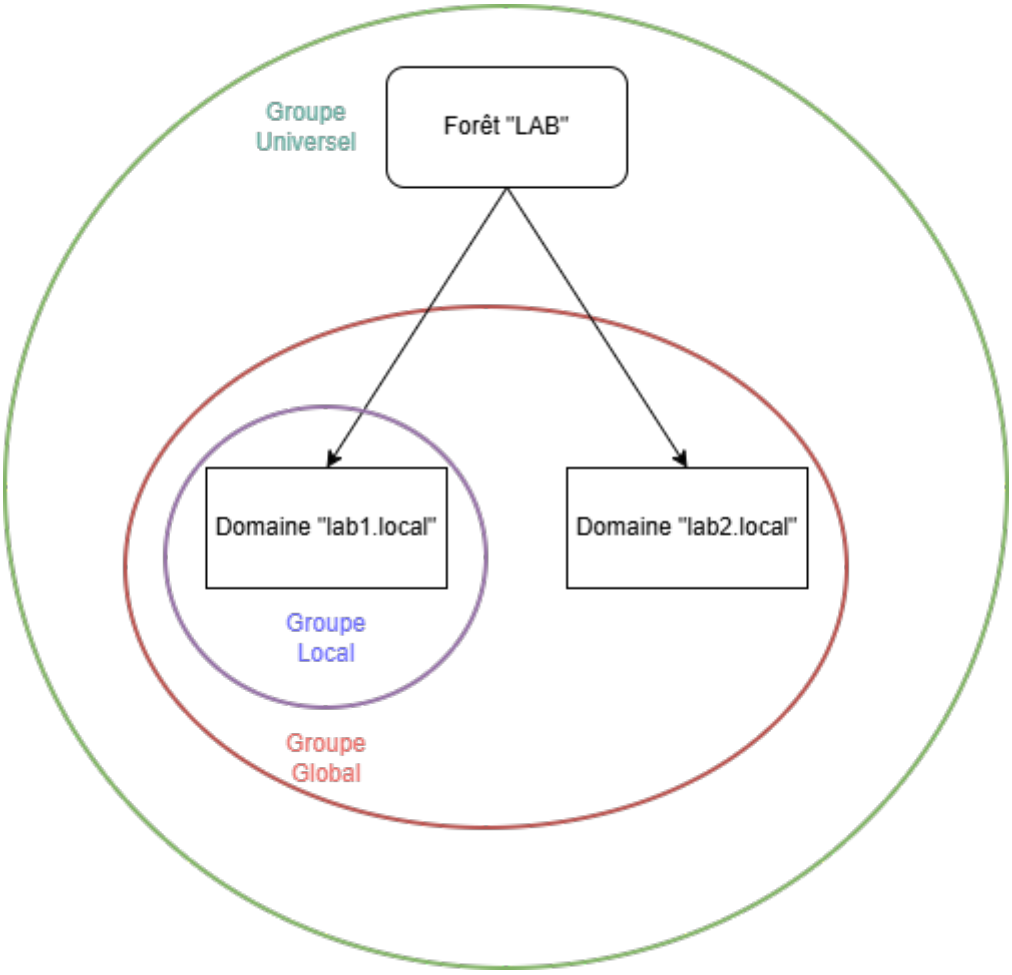
Il y a 3 niveaux de portée :

- **Domain Local** : Le groupe existe dans le domaine local. Mais n'est pas visible depuis les autres domaines.
  - Ils peuvent contenir : des utilisateurs du domaine, des groupes globaux d'autres domaines, des groupes universels.

- **Global** : Le groupe existe dans le domaine local et est visible depuis les autres domaines de la fôret.
  - Ils peuvent contenir : des utilisateurs du même domaine, des groupes globaux du même domaine.
  - Ils peuvent être membre : de groupes locaux dans n'importe quel domaine, de groupes globaux du même domaine, de groupes universel.

- **Universel** : Le groupe existe au niveau de la forêt active directory est est visible partout.
  - Ils peuvent contenir : utilisateurs de n'importe quel domaines, groupes globaux de n'importe quel domaine, autres groupes universels.

- Ils peuvent être membre : de groupes locaux dans n'importe quels domaines, d'autres groupes universels.



III. Fonctionnement de la méthode

3.1 Principe général

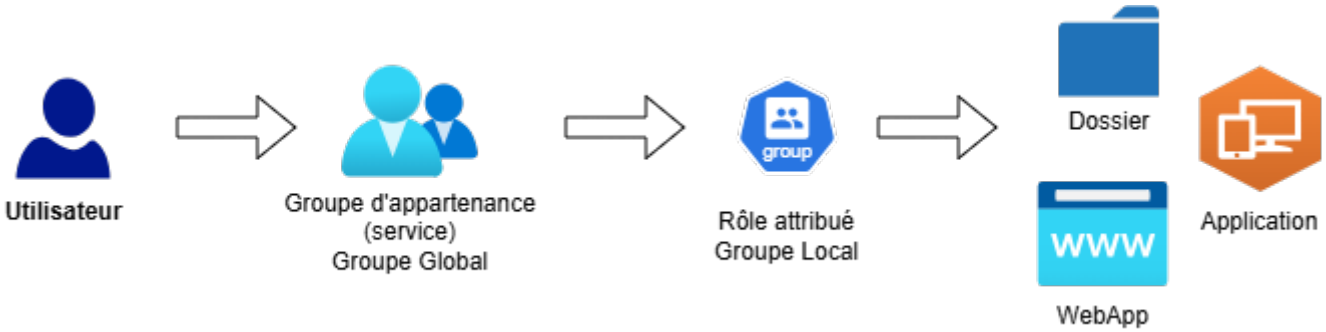
Comme vu ci-dessus, les groupes peuvent être imbriqués les uns dans les autres et c'est ce principe là qui va nous intéresser dans l'application de la méthode AGDLP.

L'idée de cette méthode est de dissocier les notions de **rôles** (droits effectifs attribué à un utilisateur) et de **groupes** d'appartenance.

Afin de limiter également la portée des droits, il faudra utiliser pour ces rôles des groupes avec une portée minimaliste.

Puis pour octroyer un rôle à un groupe d'utilisateur, il faudra ajouter le groupe des utilisateurs dans le groupe rôle.

Ainsi, si un utilisateur intègre un service dans l'entreprise, son rajout dans le groupe du service lui conférera automatiquement les accréditations (rôles) inhérents à ce service.



3.2 Normalisation

Afin de pouvoir se retrouver dans les noms et types de groupes, il va falloir adopter une normalisation stricte et une convention de nommage claire.

Les bonnes pratiques observées tendent vers la convention suivante :

- Le préfixe ***GRP*** suivi du séparateur _
- Le type de groupe (sécurité, GMSA, liste, ...)
- Un caractère de séparation. Ici _
- La ***portée*** du groupe (local, global, universel).
- Un caractère de séparation. Ici _
- La finalité de l'***utilisation*** du groupe.
- Un séparateur différent. Ici **-**
- Le ***nom*** du groupe (ou du dossier pour les groupes de sécurité).

> **Info :** les ***groupes de sécurités*** pour l'accès aux dossiers seront suffixé par ***_RO*** (read only), ***_RW*** (read-write) ou ***_FC*** (full control).

Préfixe	Type	Séparateur	Portée	Séparateur	Application	Séparateur	Usage
GRP_	SEC	_	GL	_	GPO_EXL	-	PrintServers
	GMSA		GG		GPO-INC		RDSSessionHosts
	LST		UN		RDS		Farm1
					APP		AppName
					VPN		Admins, Users
					PROXY		RestrictedUsers, Noaccess, ExtendedAccess
					VCSA		LAB1, LAB2
					FIL		Comptabilité_RO
					...		

> **Conseil** : les ***listes de distributions*** seront simplement préfixées avec '***&***' suivi du nom de la liste

GRP-GLO-RDS_AllUsers

GRP-GLO-APP_Sage

GRP-LOC-ROXY_NoInternetAccess

&ServiceComptabilité

IV. Mise en application

4.1 Appliqué au systèmes de fichiers

Exemple : Dans le cadre de son service comptabilité, l'entreprise dispose d'un partage ***//share/comptabilité***.

L'entreprise veux mettre en place 3 niveaux d'accréditation :

- Les comptables gèrent le service et doivent avoir accès en contrôle total au dossier partagé.
- Les assistants n'ont pas besoin de créer ou supprimer des choses, mais doivent pouvoir réaliser des modification dans les fichiers existants.
- Les auditeurs sont des personnes qui viennent auditer les comptes et doivent avoir un regard sur les pièces comptable, mais non pas besoin d'écrire.

Dans ce cas de figure, la première étape consiste à créer le répertoire et les groupes d'autorisations (rôles). En groupe local, car les droits ne s'appliquent que dans ce domaine.

GRP_SEC_GL_FIL_Compta_FC

GRP_SEC_GL_FIL_Compta_RW

GRP_SEC_GL_FIL_Compta_RO

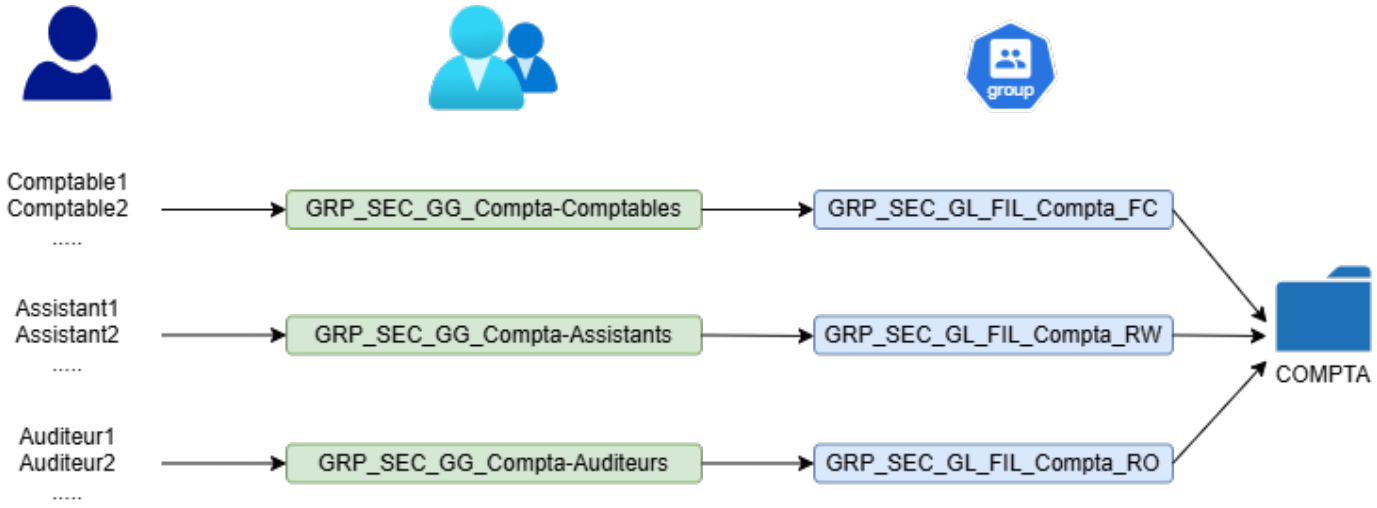
Puis créer les groupes globaux contenant les utilisateurs et les intégrer dans les groupes locaux.

GRP_SEC_GG_Compta-Comptables

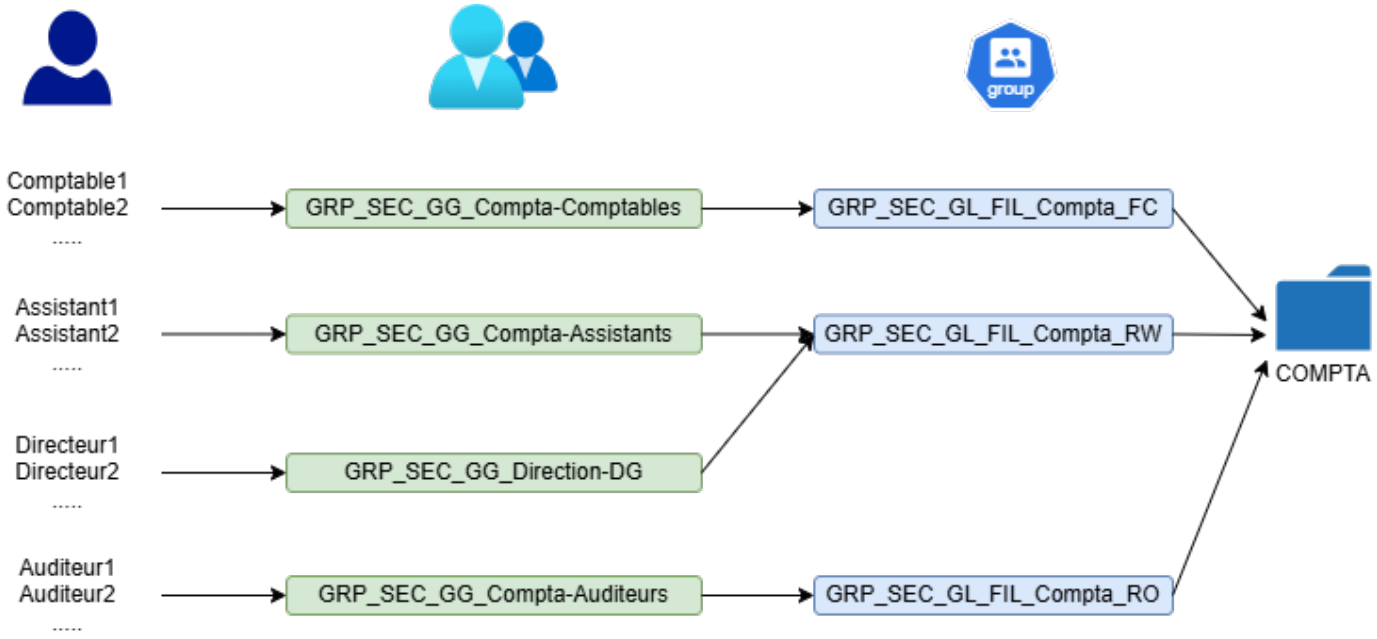
GRP_SEC_GG_Compta-Assistants

GRP_SEC_GG_Compta-Auditeurs

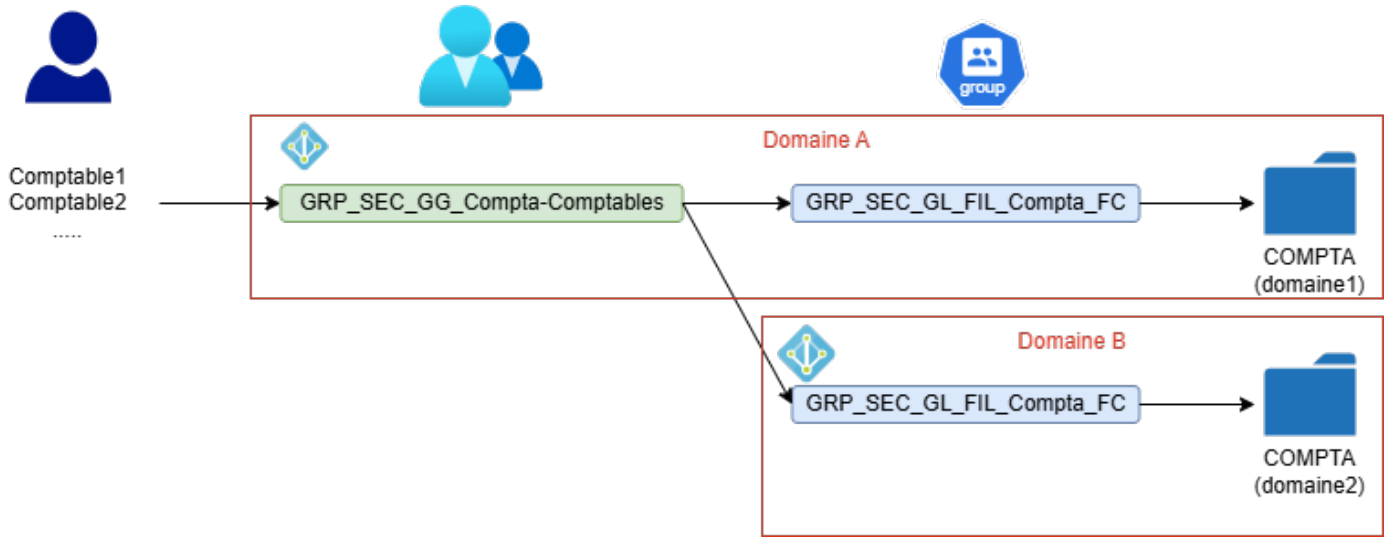
Enfin, il suffira d'ajouter / Retirer au besoin les utilisateurs dans les groupes :



Si l'on veut par exemple que le groupe Direction contenant le PDG et les membres du conseil ai également un droit de regard et de modification sur les fichiers de la comptabilité, il faudra ajouter cela de la façon suivante.



A l'inverse, si un même groupe, par exemple de comptables du siège social doit avoir accès aux dossiers comptabilité des autres domaines. Les groupes globaux étant visibles depuis les autres domaines, il faudra l'ajouter dans les groupes locaux sur les autres domaines.



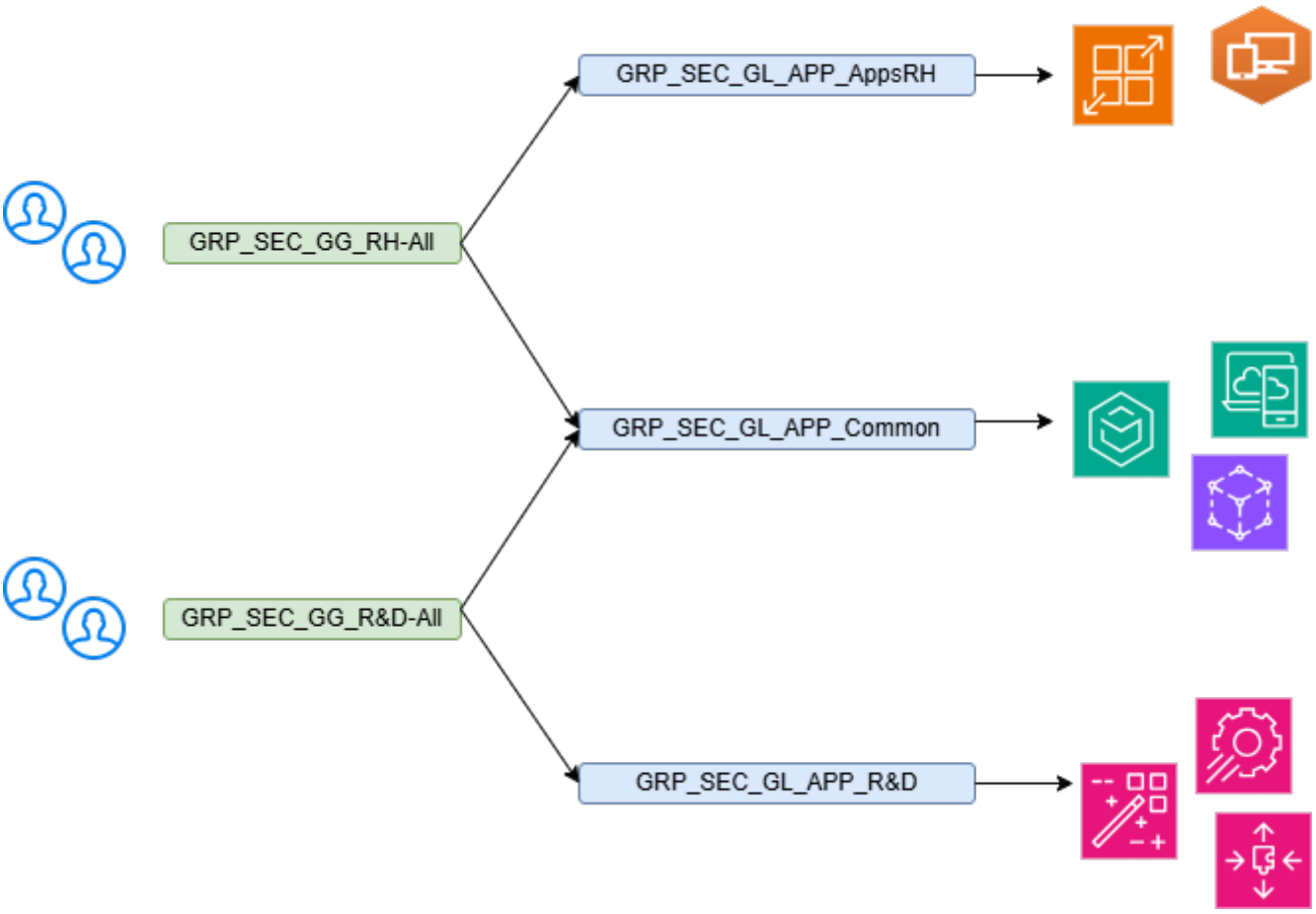
4.2 Appliqué aux applicatifs & services

Il est possible de poursuivre cette logique sur les applicatifs et services. Par exemple dans le cadre d'une ferme RDS, plusieurs applications sont partagées dans différentes collections.

Par exemple :

- le service R&D utilise un groupe d'application de conception de produits électronique en RDP.
- Le service RH utilise des application pour la gestion des bages, etc...
- Les deux services accèdent également à un pool d'applications communes à tout le personnel.

La définition se fera comme suit :



> **Info** : De même que précédemment, les groupes globaux pourront être ajouté dans des groupes locaux d'autres domaines si nécessaires. Cette méthode peut aussi s'appliquer par exemple pour des services comme le proxy, le VPN, etc...

4.3 Appliqué au SSO et aux rôles

Dans la plupart des applications modernes, la notion de rôle est déjà intégrée au sein de l'application et ce rôle peut être appliquée directement à un groupe ou utilisateur.

Ainsi il pourra être mis en place le même principe. Pour attribuer ces rôles automatiquement, cela pourra se faire de deux manières :

- Soit à travers le SSO directement qui mappera l'appartenance au groupe au rôle correspondant.
- Soit directement dans l'application, auquel cas le système reste le même que précédemment.

Le système SSO intégrera alors dans le jeton d'authentification les appartenances au groupes, ce qui permettra d'effectuer les claims (demande de rôles).

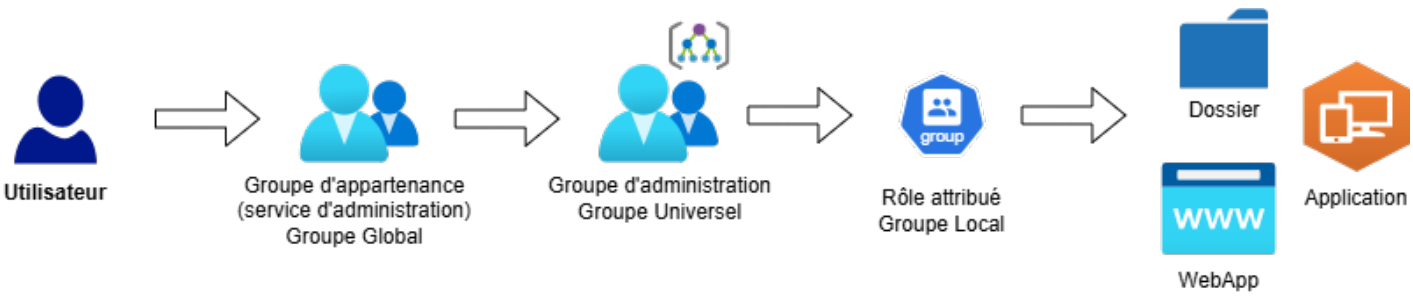
V. Variantes du modèle

5.1 AGUDLP (grosses structures)

Il s'agit de la même méthode, mais incluant également les groupes universels pour gérer les approbation sur l'ensemble des domaines.

Adapté dans un environnement multi-domaine, ou de tiering au sein d'une forêt, elle permet d'avoir par exemple un domaine d'administration et plusieurs domaines clients.

Il faudra alors ajouter les administrateurs dans un groupe global du domaine d'admin, puis ces groupes d'administration seront intégrés dans un groupe universel afin d'en faciliter l'intégration au sein des différents domaines.



5.2 AGLP

Cette variante consiste à utiliser des groupes locaux sur la machine directement au lieu d'un groupe active directory.

Cela peut être nécessaire sur des applications utilisant des groupes locaux des machines ou certains services créant eux-même des groupes locaux sur les machines afin de gérer l'accès aux ressources du services.

Ou encore certaines ressources et services sur linux.

> **Info** : Il existe également d'autres vairantes comme AGUDL P, AGUGDLP, mais celles-ci sont rare et ne constituent pas la norme de l'utilisation.

VI. Bonnes pratiques

Afin de garantir une efficacité optimale de cette méthode, il faut considérer un certain nombre de bonnes pratiques associées.

A commencer par le fait de l'intégrer dans un plan plus large. Cela va de pair avec :

- Une convention de nommage claire et explicite (comme vu ci-dessus).
- Une documentation des niveaux accréditations et une cartographie des accès.
- Une politique d'audits réguliers des groupes et permission afin de s'assurer de leur conformité.
- Mettre en place une politique de gestion du cycle de vie des groupes (validation des ajouts / suppression des membres).
- Eviter les imbrication inutiles et limiter au minimum celles-ci.
- Contrôler les délégations sur la gestion de ces groupes.

VII. Erreurs à éviter

De même que les bonnes pratiques garantissent un fonctionnement optimal, de mauvaises pratiques peuvent également venir saper l'efficacité de la méthode :

- Donner des permissions directement aux utilisateurs (bypass de la chaîne d'autorisations).
- Utiliser des groupes globaux sur les ACL (contraire au principe de moindre privilège).
- Mélanger rôles, permissions dans un même groupe.

- Ne pas nettoyer les groupes, utilisateurs, permissions obsolètes.
- Avoir une mauvaise gestion des comptes de services.

VIII. Conclusion

Si cette méthode peut ne pas être intuitive voire pénible à mettre en place, elle facilitera grandement la gestion courante des accès et des droits. Elle permettra également, sous réserve de respect des bonnes pratiques et d'éviter les erreurs, de permettre un audit rapide et efficace des accès effectifs pour un utilisateur ou un service de l'entreprise.

> **Conseil** : De plus, sa mise en oeuvre et son maintient peuvent être grandement améliorées et facilitées par la mise en place de systèmes d'automatisation à travers des scripts ou des catalogues de services IaC. Réduisant ainsi considérablement la marge d'erreur humaine et garantissant la conformité.

Revision #2
Created 2026-07-17 20:45:25 UTC by Olivier
Updated 2026-07-17 20:47:09 UTC by Olivier